WASHINGTON STATE FUSION CENTER (WSFC)

The WSFC supports activities to detect, deter, and prevent terrorism. This is accomplished through information collection, integration, analysis, reporting, and dissemination of analytical reports and other information across Federal, State, and Local government agencies, public officials, and private sector stakeholder partners.

Information Collection and Information Sharing

Suspicious activity reports are collected every day. WSFC analysts track and monitor SAR data to identify behavior or incidents that may be indicative of intelligence gathering or preoperational planning related to terrorist activity. Integration and analysis of information reported to the Fusion Center can identify criminal trends and tactics that reach beyond jurisdictional boundaries. Analysts produce timely, regionally relevant products to inform and enhance both public and private CIKR protection, preparedness, planning and response efforts. Effective information sharing between the WSFC and CIKR partners can prevent or solve crimes and even save lives.

08/2010

Partners

Pacific NorthWest Economic Region

IF YOU SEE SOMETHING, SAY SOMETHING

Report suspicious activity immediately to local authorities by calling 911

WSFC would like to receive reports for activity that falls within the identified reporting categories. This may be accomplished via:

- **Electronic interactive form at www.NWWARN.org**
- **E-mail: intake@wsfc.wa.gov**
- **WSFC Hotline: 1.877.843.9522**
- **WSFC Fax: 206.262.2014**

Washington State Fusion Center

Critical Infrastructure/Key Resources

Suspicious Activity Reporting

www.NWWARN.org
Interactive Suspicious Activity Reporting Form
WSFC Hotline — 1.877.843.9522
WSFC Fax — 206.262.2014
E-mail — intake@wsfc.wa.gov

Washington State Fusion Center

Information Sharing Environment & Suspicious Activity Reporting Categories (ISE-SAR)

Defined Criminal Activity and Potential Terrorism Nexus Activity

Breach/Attempted Intrusion

Unauthorized personnel attempting to or actually entering a restricted area or protected site. Impersonation of authorized personnel (e.g. police/security, janitor).

Misrepresentation

Presenting false or misusing insignia, documents, and/or identification, to misrepresent one's affiliation to cover possible illicit activity.

Theft/Loss Diversion

Stealing or diverting something associated with a facility/infrastructure (e.g. badges, uniforms, identification, emergency vehicles, technology or documents {classified or unclassified}, which are proprietary to the facility).

Sabotage/Tampering/Vandalism

Damaging, manipulating, or defacing part of a facility/infrastructure or protected site.

Cyber Attack

Compromising, or attempting to compromise or disrupt an organization's information technology infrastructure.

Aviation Activity

Operation of an aircraft in a manner that reasonably may be interpreted as suspicious, or posing a threat to people or property. Such operation may or may not be a violation of Federal Aviation Regulations.

Expressed or Implied Threat

Communicating a spoken or written threat to damage or compromise a facility/infrastructure.

*Potential Criminal or Non-Criminal Activity Requiring Additional Fact Information During Investigation**

Eliciting Information

Questioning individuals at a level beyond mere curiosity about particular facets of a facility's or building's purpose, operations, security procedures, etc., that would arouse suspicion in a reasonable person.

Testing or Probing of Security

Deliberate interactions with, or challenges to, installations, personnel, or systems that reveal physical, personnel or cyber security capabilities.

Photography

Taking pictures or video of facilities, buildings, or infrastructure in a manner that would arouse suspicion in a reasonable person. Examples include taking pictures or video of infrequently used access points, personnel performing security functions (patrols, badge/vehicle checking), security-related equipment (perimeter fencing, security cameras), etc.

Observation/Surveillance

Demonstrating unusual interest in facilities, buildings, or infrastructure beyond mere casual or professional (e.g. engineers) interest such that a reasonable person would consider the activity suspicious. Examples include observation through binoculars, taking notes, attempting to measure distances, etc.

Recruiting

Building of operations teams and contacts, personnel data, banking data or travel data.

Materials Acquisition/Storage

Acquisition and/or storage of unusual quantities of materials such as cell phones, pagers, fuel, chemicals, toxic materials, and timers, such that a reasonable person would suspect possible criminal activity.

Acquisition of Expertise

Attempts to obtain or conduct training in security concepts; military weapons or tactics; or other unusual capabilities that would arouse suspicion in a reasonable person.

Weapons Discovery

Discovery of unusual amounts of weapons or explosives that would arouse suspicion in a reasonable person.

Sector-Specific Incident

Actions associated with a characteristic of unique concern to specific sectors (such as the public health sector), with regard to their personnel, facilities, systems or functions.

***Note:** *These activities are generally First Amendment-protected activities and should not be reported in a SAR or ISE-SAR absent articulable facts and circumstances that support the source agency's suspicion that the behavior observed is not innocent, but rather reasonably indicative of criminal activity associated with terrorism, including evidence of pre-operational planning related to terrorism. Race, ethnicity, national origin, or religious affiliation should not be considered as factors that create suspicion (although these factors may be used as specific suspect descriptions).*

Intake Hotline: 1.877.843.9522 ***Email: intake@wsfc.wa.gov***